REMARKS

Applicant has made clarifying amendment to claim 1 to change "with" to –to--, clarifying that the gateway communicates the statistics to the control center and has moved material from the preamble into the body of the claim. No new consideration is required of these changes since the change of "with" to –to-- is typographical in nature and a similar limitation of "the gateway communicating statistics to the control center" is found in independent claims 16 and 29 and moving of the material from the preamble was presumably already considered by the examiner.

Applicant has also amended claim 16 to delete the step of disposing a gateway ... .

The examiner rejected claims 1-39 under 35 U.S.C. 102(e) as being anticipated by Yavatkar, et al. (US 6,735,702).

The examiner stated:

> **As per claim 1:**
> **discloses gateway device disposed between a data center and a network for thwarting denial of service attacks on the data center, the gateway device comprises: a computing device comprising:**
> **a monitoring process that monitors network traffic through the gateway; [col. 1, lines and col.7, lines 43-48]**
> **a communication process that communicate statistics collected [col.2, lines 4-5 and 53-60 and col.3, lines 28-45; statistics from the monitoring process is inherently gathered data of similarities or differences used for analysis purposes to determine the attacks and kind of traffic on the gateway.] in the gateway from the monitoring process with a control center and that receives queries or instructions from the control center; [col.3, lines 25-29 and col. 11, lines 51-55] and**
> **a filtering process to insert filters on network devices [col.3, lines 46-53 and col. 13, lines 56-62] to filter out packets that the gateway deems to be part of an attack. [col.20, lines 20-21] (Emphasis in original omitted)**

Claim 1 is patentable distinct over Yavatkar et al. since Yavatkar et al neither describes nor suggests "A gateway device comprising a computing device, disposed between a data center and a network for thwarting an attack on the data center, the computing device executing a monitoring process ... a communication process that communicates statistics collected in the gateway by the monitoring process to a control center and that receives queries or instructions from the control center."

Claim 1 further distinguishes since Yavatkar fails to describe or suggest that the gateway includes a filtering process to insert filters on network devices to filter out packets that the gateway or the control center deems to be part of an attack.

Yavatkar et al. fail to disclose or suggest the claimed gateway device. In particular, Yavatkar fails to describe that the gateway includes a computing device, disposed between a data center and a network and the computing device executing a monitoring process ... a communication process and a filtering process, as claimed. The examiner pieces elements from Yavatkar et al, that exist in three separate unrelated mechanisms in Yavatkar to concoct the claimed gateway. For example, the monitoring process the examiner finds in [col. 1, lines and col.7, lines 43-48. Col. 1 is a prior art discussion and therefore would not be includied in any device that Yavatkar were to describe. Col 7 lines 43-48 pertains to discussion of a gateway. Specifically Yavatkar discloses that: "Node 48 is a gateway, providing network 4 access to other networks, such as the Internet, and acting as a firewall. Link 84 transmits data between node 48 and other networks." However, that gateway is not described as performing any of the claimed functions.

For the communication process Yavatkar relies on col.2, lines 4-5, which is a discussion of a prior art "sniffer." and 53-60, which is a discussion of his inventive concept, which does not indicate any use for the "sniffer." Similarly col.3, lines 28-45 is a discussion of two different mobile agents that collect data on the state of the network.

For the filtering process to insert filters on network devices the examiner relies on col.3, lines 46-53 discussion of watchdog and bloodhound agents and col. 13, lines 56-62 discussion of a gateway that can be shut down or have filters installed. While Yavatkar does mention a prior art method, at Col. 13, namely:

> **However, using current methods to identify the gateway which is, in effect, the source of attack traffic to the network can be difficult and time consuming. A network administrator using a sniffer may determine which physical link (of multiple links) on a device receiving attack traffic is the source of such traffic. Certain modules resident on nodes may perform similar functions under the direction of a central console. With such information a network administrator may move from node to node, tracing the path of the hostile messages from the victim to the source, or to the gateway allowing such traffic to enter the network. Such a method of determining the source of messages is slow.**

Yavatkar teaches away from any combination of a "sniffer" device arguing that it is a conventional method and is slow.

The teachings that the examiner relies on in Yavatkar are to elements that area on different devices. The devices perform somewhat similar, but not identical functions, as the claimed gateway. However, the claimed gateway is a computing device that performs all of the functions recited. Yavatkar does not show any device that performs all of the recited functions. Therefore, for this reason alone, Yavatkar is not an anticipating reference since Yavatkar fails to describe a device that possess all of the recited features.

The examiner also argues that: "statistics from the monitoring process is (sic) inherently gathered data of similarities or differences used for analysis purposes to determine the attacks and kind of traffic on the gateway." Applicant disagrees. With respect to the "sniffer" device Yavatkar teaches the prior art technique as slow and inaccurate. According to Yavatkar:

> **For example, to determine the node which is the source of attack traffic (or the gateway allowing such traffic into a network, which in such a case may be considered a source) and the path or paths taken by such traffic, a human operator may access each link at a node receiving such traffic and analyze the incoming traffic using a sniffer. A sniffer is a device which may record network statistics at a node. The operator may identify which of the physical links attached to the node is receiving a certain type or amount of traffic and then move to the node on the other end of the identified link. The path or paths of traffic from the source of the traffic may be found by traversing the network from node to node, using the sniffer at each node in a path, until the source is reached.**

The disclosed sniffer may record network statistics at a node. However, it is the operator that may identify which physical link attached to the node received a certain type or amount of traffic and then move to the node on the other end of the link. However, this does not teach the features of a monitoring process that monitors network traffic through the gateway and a communication process that communicates statistics collected in the gateway by the monitoring process to a control center and that receives queries or instructions from the control center. Thus, for these reasons and the reasons of record claim 1 is allowable over the art.

Claim 1 also requires a filtering process to insert filters on network devices to filter out packets that the gateway or the control center deems to be part of an attack.

Yavatkar however teaches to shut down the gateway or to insert filters. However, in Yavatkar, that decision is performed by an administrator using a sniffer that determines a

physical link or certain modules under direction of a central console, not as in claim 1 where a computing device includes a filtering process the filter removes packets that the gateway deems to be part of the attack. Yavatkar also discloses that with such information a network administrator moves from node to node, tracing the path of the hostile messages from the victim to the source or to the gateway allowing such traffic to enter the network. Yavatkar acknowledges that such a method of determining the source of messages is slow. Yavatkar proposes to address this by use of watchdog and bloodhound agents discussed starting at Col. 14, line 18. Therefore, Yavatkar fails to teach to insert filters to filter out packets that the gateway deems to be part of an attack.

Claims 2-15 are allowable at least for the reason that they depend directly or indirectly on claim 1. These claims are also allowable for the reasons discussed of record.

Claim 16, as amended recites monitoring network traffic through a gateway ... and measuring heuristics ... to provide statistics on the network traffic, communicating the statistics ... to a control center and filtering out packets that the gateway or control center deems to be part of an attack. For analogous reasons as discussed in claim 1, claim 16 is allowable.

Claims 17-28 are allowable at least for the reason that they depend directly or indirectly on claim 16. These claims are also allowable for the reasons discussed of record.

Claim 29 is directed to a computer program product ... to monitor network traffic sent to the victim site and measure heuristics of the network traffic to provide statistics on the network traffic, communicate statistics collected in the computer device to a control center, and filter out packets that the device or control center deems to be part of an attack.

For analogous reasons as discussed in claim 1, claim 29 is allowable.

Claims 30-39 are allowable at least for the reason that they depend directly or indirectly on claim 29. These claims are also allowable for the reasons discussed of record.

Canceled claims, if any, have been canceled without prejudice or disclaimer.

Any circumstance in which the applicant has (a) addressed certain comments of the examiner does not mean that the applicant concedes other comments of the examiner, (b) made arguments for the patentability of some claims does not mean that there are not other good reasons for patentability of those claims and other claims, or (c) amended or canceled a claim

does not mean that the applicant concedes any of the examiner's positions with respect to that claim or other claims.

Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 6/27/06

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

21364108.doc